Pearson BTEC Level 3 Nationals Diploma, Extended Diploma

Window for supervised period:
Monday 24 April 2023 – Monday 15 May 2023

Supervised hours 4 hours

Paper reference **20158K**

Information Technology

UNIT 11: Cyber Security and Incident Management

Part B

You must have:
Forensic_Analysis.rtf

Instructions

- **Part A** and **Part B** contain material for the completion of the set tasks under supervised conditions.
- There are 43 marks for **Part A** and 37 marks for **Part B**, giving a total mark for the set tasks of 80.
- **Part A** and **Part B** are specific to each series and this material must be issued only to learners who have been entered to take the tasks in the specified series.
- Learners **must only** have access to **Part B** during this supervised assessment period.
- This booklet should be kept securely until the start of the 4-hour, **Part B** supervised assessment period.
- **Part A** will need to have been completed and kept securely before starting **Part B**.
- **Part A** materials must not be accessed during the completion of **Part B**.
- Both parts will need to be completed during the 3-week period timetabled by Pearson.
- **Part A** and **Part B** tasks must be submitted together for each learner.
- This booklet should not be returned to Pearson.
- Answer **all** activities.

Information

- The total mark for this Part is 37.

Turn over ▶

©2023 Pearson Education Ltd.

Pearson

Instructions to Invigilators

This paper must be read in conjunction with the unit information in the specification and the *BTEC Nationals Instructions for Conducting External Assessments (ICEA)* document. See the Pearson website for details.

Refer carefully to the instructions in this task booklet and the *BTEC Nationals Instructions for Conducting External Assessments (ICEA)* document to ensure that the assessment is supervised correctly.

Part A and **Part B** set tasks should be completed during the period of 3 weeks timetabled by Pearson. **Part A** must be completed before starting **Part B**.

The 4-hour **Part B** set task must be carried out under supervised conditions.

The set task can be undertaken in more than one supervised session.

An electronic template for activity 4 is available on the website for centres to download for learner use.

Learners must complete **Part B** on a computer using the template provided and appropriate software. All work must be saved as PDF documents for submission.

Invigilators may clarify the wording that appears in **Part B** but cannot provide any guidance in completion of the task.

Invigilators should note that they are responsible for maintaining security and for reporting issues to Pearson.

Maintaining Security

- Learners must not bring anything into the supervised environment or take anything out.
- Centres are responsible for putting in place appropriate checks to ensure that only permitted material is introduced into the supervised environment.
- Internet access is not permitted.
- Learners' work must be regularly backed up. Learners should save their work to their folder using the naming instructions indicated in each activity.
- During any permitted break, and at the end of the session, materials must be kept securely, and no items removed from the supervised environment.
- Learners can only access their work under supervision.
- User areas must only be accessible to the individual learners and to named members of staff.
- Any materials being used by learners must be collected in at the end of each session, stored securely and handed back at the beginning of the next session.
- Following completion of **Part B**, all materials must be retained securely for submission to Pearson.
- **Part A** materials must not be accessed during the completion of **Part B**.

Outcomes for Submission

Each learner must create a folder to submit their work.

The folder should be named according to this naming convention:

[Centre #]_[Registration number #]_[surname]_[first letter of first name]_U11B

Example: Joshua Smith with registration number F180542 at centre 12345 would have a folder titled

12345_F180542_Smith_J_U11B

Each learner will need to submit 2 PDF documents within their folder.

The 2 PDF documents should use these file names:

Activity 4: activity4_incidentanalysis_[Registration number #]_[surname]_[first letter of first name]

Activity 5: activity5_securityreport_[Registration number #]_[surname]_[first letter of first name]

An authentication sheet must be completed by each learner and submitted with the final outcomes.

The work should be submitted no later than 15 May 2023.

Instructions for Learners

Read the set task information carefully.

Plan your time carefully to allow for the preparation and completion of all the activities.

Your centre will advise you of the timing for the supervised period. It is likely that you will be given more than one timetabled session to complete these tasks.

Internet access is **not** allowed.

You will complete this set task under supervision and your work will be kept securely at all times.

You must work independently throughout the supervised assessment period and must not share your work with other learners.

Your invigilator may clarify the wording that appears in this task but cannot provide any guidance in completion of the activities.

Part A materials must not be accessed during the completion of **Part B**.

Outcomes for Submission

You must create a folder to submit your work.

The folder should be named according to this naming convention:

[Centre #]_[Registration number #]_[surname]_[first letter of first name]_U11B

Example: Joshua Smith with registration number F180542 at centre 12345 would have a folder titled

12345_F180542_Smith_J_U11B

You will need to submit 2 PDF documents within this folder.

The 2 PDF documents should use these file names:

Activity 4: activity4_incidentanalysis_[Registration number #]_[surname]_[first letter of first name]

Activity 5: activity5_securityreport_[Registration number #]_[surname]_[first letter of first name]

You must complete an authentication sheet before you hand your work in to your invigilator.

Set Task Brief

The Eighties Hotel

Peter Okdekaj is the owner of a hotel chain, Okdekaj Hotels Group (OHG). Each hotel is themed on different historical periods, e.g. Edwardian or Victorian.

Peter has recently purchased another building that he is going to develop into a hotel themed on the 1980s.

The building was constructed in 1985. It is a six-floor apartment block. There is a shopping arcade on the ground floor, an underground car park and five accommodation floors. The original facade and car park will be kept, and the apartments will be converted to hotel rooms. The ground floor shopping arcade will be made into offices, a reception area, a restaurant, and other public amenities.

In keeping with the Eighties theme:

- no wireless communication is available in the hotel except for short range systems required for contactless payments
- each guest room has an entertainment centre that provides 1980s films, music, TV programmes and computer facilities.

As WiFi and the internet were not available before the 1990s, there will not be any guest WiFi in the hotel and the internet will only be available through guests' own devices.

The 1980s computer facilities are supplied by virtual machines running on a dedicated server. These virtual machines emulate IBM compatible 386 machines from 1986. They would have been high end, home PCs at the time.

The operating system is Microsoft Disk Operating System (MS-DOS) version 3.2 MS-DOS 3.2 uses a command line interface and was introduced in 1986. It allows networking and supports 3.5-inch, 720 KB floppy drives.

Peter has many years of experience in hotel management but thinks of himself as an IT user rather than an IT specialist. He relies on OHG's IT staff to run the network.

Client brief

You advised Peter on cyber security matters when the hotel was being planned. Now, a few months later, he has asked you to review the investigation of a cyber security incident.

The incident occurred during the first weekend in May.

A guest reported that the computer in their entertainment system had done something peculiar. The text in the MS-DOS interface had suddenly started to drop letters to the bottom of the screen. When everything had fallen, the message "Hello from 1988. Your computer is now infected." appeared.

The duty technician realised that this was a potential system breach and started an incident report.

Evidence items from the security incident at OHG's Eighties Hotel

Evidence items include:

1. Network Manager's report
2. Virus history
3. Files used in the emulated 386 machine
4. Network diagram
5. Addendum to Network Manager's report
6. Cyber security document – incident management policy.

1. Network Manager's report

Sun. 7th May. 2023. 17:00

Hennrick Bello: Network Manager, Eighties Hotel: OHG

Cyber security incident report. Incident Number 20230052

Team members

Hennrick Bello: Network Manager
Jade Rolle: Deputy Network Manager (senior on site technician)

Situation

Jade Rolle, our Deputy Network Manager was on duty on Saturday 6th May. She responded to a guest report, logged at 18.36, that the 1980s computer was behaving strangely.

The guest reported that they had been logged in and had the GAME directory showing when the text started to fall down the screen and accumulate at the bottom. This took about thirty seconds to empty the screen. A message was then displayed saying

"**Hello from 1988. Your computer is now infected**"

Jade visited the guest's room and confirmed that the message was as described.

The computer would not react to the keyboard until Jade used ctrl-alt-del to try and stop whatever was causing the effect. The computer then returned to normal operation, showing the Command Prompt C:\GAME>_

The guest stated that they had been playing the games but had not touched any of the other applications. Jade made a copy of the files that might have been used by the guest. **(See evidence item 3).** She also cloned the virtual machine in its current state for further investigation.

Further use of the computer failed to recreate the falling text effect.

There had been no other reports from guests of anything similar.

Jade performed an internet search for "Hello from 1988. Your computer is now infected". An exact match was not found but a similar message was associated with the Stoned virus.

Further searching showed that the falling text behaviour was associated with the Cascade virus. Both Stoned and Cascade are 1980's viruses.

Jade compiled some notes about them for reference. **(See evidence item 2)**

Jade thought that the incident was unusual so she telephoned me at 19:40 to discuss the matter. With no further incidents being reported and a simple fix via ctrl-alt-del, I told her to log the incident as minor but said we'd activate the Computer Security Incident Response Team (CSIRT) and would look at it further the next day.

I logged the activation of the CSIRT at 19:45 on Sat 6th May.

The investigation

The CSIRT met at 09:00 on Sun 7th May to consider the incident.

Team members present; Hennrick Bello: Team Leader, Jade Rolle: Deputy Network Manager.

The team determined that there was no possibility that guest or company data could have been compromised, and no further team members needed to be co-opted at that stage.

Material available:
- Preliminary notes.
- Copy of files **(See evidence item 3)**

Cloned virtual machine.

On reading Jade's notes about the Stoned and Cascade viruses, it was obvious that the incident could not have been caused by one of/a combination of them. The team therefore looked at other possibilities.

1. An infection brought in by the guest.
2. An infection in the files used by the virtual machine server.
3. An undocumented feature in one of the pieces of 1980's software.

1. Was rejected as the guest did not have a floppy disk and had not asked for an adaptor to use with an SD card.

2. Was checked by running an anti-malware scan on the files. Nothing was detected. Specific checks for signatures of Stoned and Cascade were also negative.

3. This remains a possibility but is difficult to prove/disprove based on a single incident. An internet search did not produce any similar situations.

The team looked at the game files that had been used **(See evidence item 3).** On the assumption that the Cascade part was mimicking the original virus, it was deemed very unlikely that a game was involved.

The team looked at the DOS files being used. Nothing obvious was seen and it appeared that the only way to check would be to try all the possible DOS commands to see if any were broken. This proved ineffectual as several commands could not work in the virtual environment.

The team then downloaded some other copies of DOS 3.2 from the internet in order to match files against the ones present. This was also ineffectual as, at that time (1980s), each manufacturer seemed to have its own version of DOS. Sometimes different versions, for each model of computer. In addition, while the file sizes in different versions were often the same, this was not always the case.

The cloned virtual machine was then investigated but no actions by the team could replicate the event.

<u>Conclusions</u>

In the absence of anti-malware results or further similar incidents, no firm conclusion could be reached.

Remedial action

As a precaution, all files for DOS 3.2 games, and other applications were replaced with versions downloaded from different sources.

The incident was closed at 17:00 Sun 7th May.

Addendum to Network Manager's report

An unofficial investigation into the possibility of an undocumented feature was conducted.

(See evidence item 5)

2. Virus history

Stoned virus

- Invented in New Zealand in 1987, became distributed worldwide in 1988.
- Boot sector virus, carried by floppy disks.
- Infects the master boot sector of the hard disk.
- Only tries infecting other floppy disks when the floppy drive is running.
- Tests the boot sector for infection and does not attempt to access infected disks.
- Prints a message depending on the value of one bit in the computer's internal clock. One in eight chance of appearing.
- No other effects on the running of the computer.

Cascade virus

- Invented in Germany in 1987, became distributed worldwide in 1988.
- Infects .COM files by changing the first three bytes of the .COM file code to point to the virus file. The file length remains the same, making detection more difficult.
- When an infected .COM file is run, Cascade moves into memory and becomes resident.
- The resident virus will infect other .COM files as they are run.
- Cascade causes the characters on a DOS screen to randomly cascade to the bottom of the screen to form a pile of numbers and letters.
- The file that causes the cascade behaviour is runnable and will be .EXE .COM or .SYS. It may hide by replacing a genuine file.
- It was originally written to execute when an infected file is run between October 1 and December 31 in 1988.

3. Files used in the emulated 386 machine

Files in C:\DOS>

The version used in the Eighties Hotel is shown in the first column, an IBM DOS written for a generic 386 machine. The other columns show versions of DOS written for three other computer manufacturers.

IBM5170	NEC Powermate Portable APC IV	Olivetti Personal Computer	Tandy 1000TX OEM	
ANSI.SYS	ANSI.SYS	ANSI.SYS	ANSI.SYS	MLPART.COM
APPEND.COM	ASSIGN.COM	COMMAND.COM	APPEND.COM	LINK.EXE
ASSIGN.COM	ATTRIB.COM	COUNTRY.SYS	ASSIGN.COM	LPDRVT.SYS
ATTRIB.COM	BACKUP.EXE	DISPLAY.SYS	ATTRIB.EXE	MLPART.SYS
BACKUP.EXE	CHKCMOS.EXE	DRIVER.SYS	AUTOFMT.EXE	MODE.COM
CHKDSK.EXE	CHKDSK.EXE	FASTOPEN.EXE	BACKUP.COM	MORE.COM
CLOCK.SYS	COMMAND.COM	FDISK.COM	CACHE.COM	MOUSE.COM
COMMAND.COM	COMP.COM	FORMAT.COM	CHKDSK.COM	MOUSE.SYS
DISKCOMP.COM	CONFIG.SYS	KEYB.COM	COMMAND.COM	PATCH.COM
DISKCOPY.COM	DISKCOMP.COM	KEYBOARD.SYS	CPANEL.COM	PRINT.COM
DRIVER.SYS	DISKCOPY.COM	MODE.COM	DC.COM	RCRYPT.COM
EDLIN.EXE	DRIVER.SYS	NLSFUNC.EXE	DEBUG.COM	RECOVER.COM
EXE2BIN.EXE	EDLIN.EXE	PRINTER.SYS	DISKCOMP.COM	REPLACE.EXE
FC.EXE	EXE2BIN.EXE	REPLACE.EXE	DISKCOPY.COM	RESTORE.COM
FDISK.EXE	FC.EXE	SELECT.COM	DISKOPT.COM	SELECT.COM
FIND.EXE	FDISK.EXE	SYS.COM	DISKTYPE.COM	SHARE.EXE
FORMAT.EXE	FIND.EXE	VDISK.SYS	EDLIN.COM	SHIPTRAK.COM
GRAFTABL.EXE	FORMAT.COM	XCOPY.EXE	EXE2BIN.EXE	SORT.EXE

IBM5170	NEC Powermate Portable APC IV	Olivetti Personal Computer	Tandy 1000TX OEM	
GRAPHICS.EXE	GRAFTABL.COM	EGA.CPI	FBACKUP.COM	SPOOLER.COM
IO.SYS	GRAPHICS.COM	LCD.CPI	FC.EXE	SPOOLER.SYS
JOIN.EXE	IO.SYS	4201.CPI	FDISK.COM	SUBST.EXE
KEYBDV.EXE	JOIN.EXE	5202.CPI	FIND.EXE	SYS.COM
KEYBSP.EXE	KEYBUK.COM		FORMAT.COM	TREE.COM
KEYBUK.EXE	LABEL.COM		FRESTORE.COM	VDISK.SYS
LABEL.EXE	LINK.EXE		GRAPHICS.COM	XCOPY.EXE
LINK.EXE	MODE.COM		HSECT.COM	
MODE.EXE	MORE.COM		IBMBIO.COM	
MORE.COM	PRINT.COM		IBMDOS.COM	
PRINT.EXE	RECOVER.COM		JOIN.EXE	
RAMDRIVE.SYS	REPLACE.EXE		KEYCNVRT.SYS	
RECOVER.EXE	RESTORE.COM		KEYTFR.COM	
REPLACE.EXE	RETRACT.EXE		KEYTGR.COM	
RESTORE.EXE	SELECT.COM		KEYTSP.COM	
SHARE.EXE	SHARE.EXE		KEYTUK.COM	
SORT.EXE	SORT.EXE		LABEL.COM	
SUBST.EXE	SUBST.EXE		LF.COM	
SYS.COM	SYS.COM		LIB.EXE	
TREE.EXE	TREE.EXE		LPSETUP.COM	
XCOPY.EXE	XCOPY.EXE		MLFORMAT.COM	

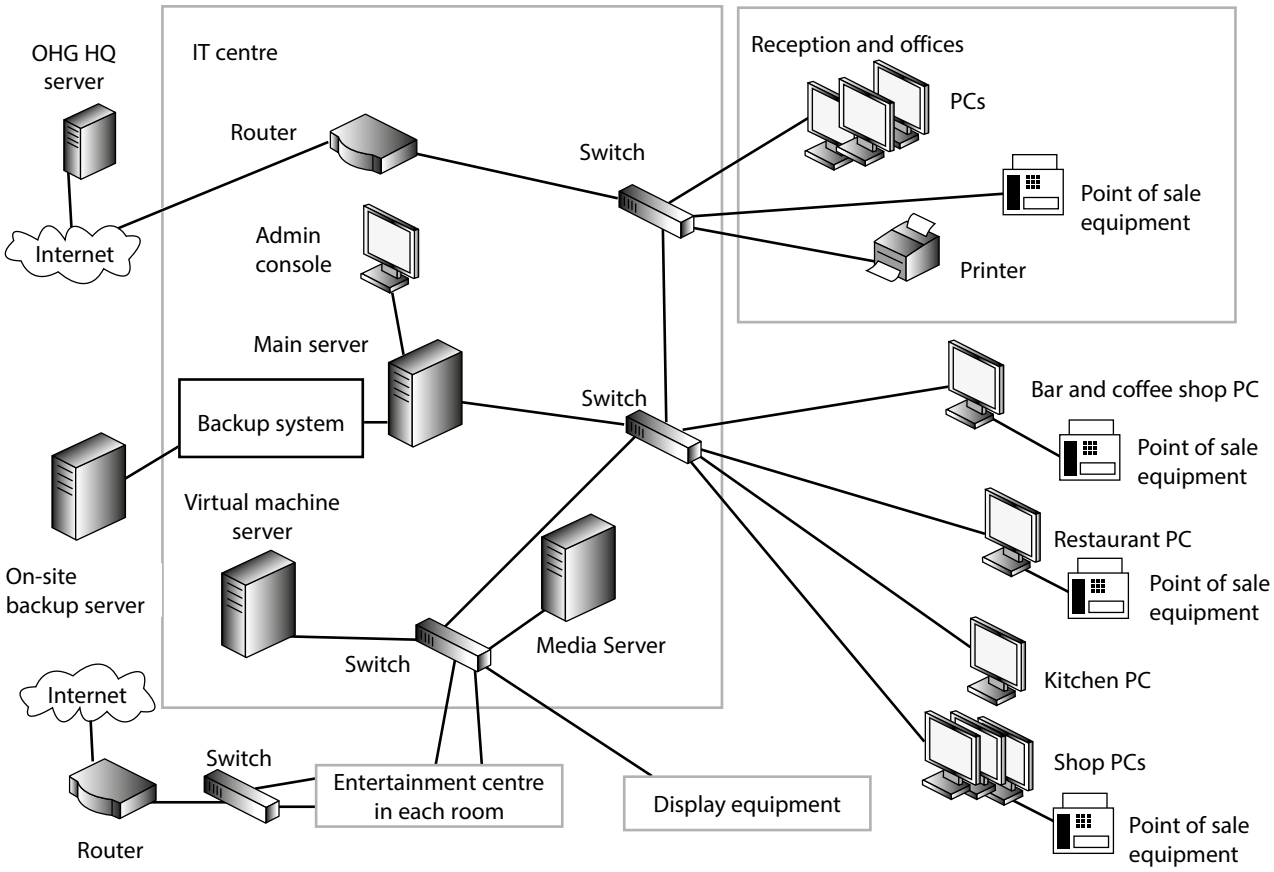
Files in C:\GAMES>

Files for the games played by the guest prior to the Stoned/Cascade event.

All the games worked correctly when tested after the event.

Chess	Kong	PacMan	Titanic	Turbo Racer
CHESS.EXE	KONG.BIN	BAKGND	BEYOND.COM	TURBO.BAT
CHESS1.OVL	KONG.EXE	EATDOT	BEYOND.000	TURBO.EXE
CHESS2.OVL		EATFR	BEYOND.001	
CHESS3.OVL		EATGH	INSTRUCT.BAT	
CHESS4.OVL		EXLIFE	LINE	
CHESS5.OVL		FRT*	ROOMS1	
CHESS6.OVL		M1	ROOMS2	
CHESS7.OVL		M2	SPECIAL1	
PSION.GRT		M3	SPECIAL2	
		MSPAC.EXE		
		PACDIE		
		POWERUP		
		POWUP2		
		TITLE		

4. Network diagram



5. Addendum to Network Manager's report

Sat. 13th May. 2023

Re: Cyber security incident report. Incident Number 20230052

Following the closure of the incident on 7th May 2023, I told my daughter, Adele, about the incident. She is studying for a Computer Science degree. She asked if she could have a look at the preserved files. OHG agreed so I gave her a copy.

Adele installed an emulator on her laptop. She then ran numerous scenarios to try and replicate the event.

A breakthrough came after she left her laptop unattended for a while. On her return "**Hello from 1988. Your computer is now infected.**" was displayed.

Adele hypothesised that the behaviour required a timed interval of inactivity. She set up several virtual machines and tried to replicate the event again.

Results

1. The waiting period was exactly 33 minutes 8 seconds.

2. It did not matter which games or other applications, if any, were used before the inactivity.

3. The event only happened in about 10% of the trials.

Conclusions

Adele thinks that the only way to solve the problem would be to disassemble all the files into their original assembly language and see which contains the code for the message.

6. Cyber security document – incident management policy

Incident management team

The Computer Security Incident Response Team (CSIRT) shall consist of:

- The Network Manager at the Eighties Hotel (Team Leader)
- The Senior Technician present at the time of the incident.

If the Team Leader suspects that customer data may have been compromised, representatives of the OHG Legal and Public Relations teams shall be co-opted.

The Team Leader shall co-opt other team members as needed.

Incident reporting

Any member of staff who considers that an IT-related security incident has occurred must report it as soon as possible to the Team Leader.

Initially it may be reported verbally but this must be followed up by an email. It is the responsibility of the CSIRT to maintain detailed documentation on the incident from first report to final resolution.

Security incidents may include:

- theft of IT equipment
- theft of company data
- unauthorised access to the Eighties Hotel systems
- infection of the Eighties Hotel systems with malware.

Incident response procedures

(a) Theft of IT equipment

- Theft of IT equipment is a very serious issue. Any thefts must be reported at once to the CSIRT Leader, initially a verbal report must be made followed up by email, providing as much information as possible (location and type of equipment, when it was last seen etc.).
- The CSIRT Leader must ascertain if the item has actually been stolen (or if it is just missing).
- If the item is confirmed as stolen, the CSIRT Leader must inform OHG finance department so they can inform insurers.
- The CSIRT must prepare a report on the theft for the Eighties Hotel Manager, and if needed justify the finances required to replace the stolen item.

(b) Theft of data

- Theft or loss of data may occur in a number of different ways.
- Any loss of data must be reported at once to the CSIRT Leader, initially a verbal report must be made followed up by email.
- The CSIRT must investigate the loss and identify exactly what data has been lost or stolen and when the incident occurred.
- Where it is suspected that customers' personally identifiable information has been accessed, a report must be made to the Eighties Hotel Manager, who will then report to OHG HQ.
- Having identified what has been lost or stolen, and when, the CSIRT must retrieve backups and restore the data as soon as possible.
- The CSIRT should review the incident and implement procedures to prevent future losses.

(c) Infection of IT systems with malware

- Any member of staff who suspects that any system has been infected with malware must report at once to the CSIRT Leader, initially a verbal report must be made followed up by email.
- The infected system should be shut down as soon as possible
- The CSIRT will investigate the infection and take appropriate measures to resolve the infection and restore the system.

(d) Unauthorised access to systems

- Any member of staff who suspects that there has been unauthorised access to any system must report it at once to the CSIRT Leader, providing as much detail as possible (which system, how access was obtained). Initially a verbal report must be made, followed up by email.
- The CSIRT will thoroughly investigate the incident and identify how the unauthorised access was obtained.
- The CSIRT will take whatever action is required to prevent future occurrences (e.g. change passwords).

Part B Set Task

You must complete ALL activities within the set task.

Produce your documents using a computer.

Save your documents in your folder ready for submission using the formats and naming conventions indicated.

Read the set task brief carefully before you begin and note that reading time is included in the overall assessment time.

You have been advising Peter Okdekaj on cyber security. Now he has asked you to review the investigation of a cyber security incident.

Activity 4: Forensic incident analysis

Analyse the forensic evidence, including how the evidence was obtained, for the cyber security incident at OHG's Eighties Hotel.

Consider possible causes of the incident and come to a conclusion about the most likely cause of the incident.

Refer to evidence items 1–5 inclusive.

Produce a forensic incident analysis using the template **Forensic_Analysis.rtf**

Save your completed forensic incident analysis as a PDF in your folder for submission as **activity4_incidentanalysis_[Registration number #]_[surname]_[first letter of first name]**

You are advised to spend 2 hours on this activity.

(Total for Activity 4 = 14 marks)

Activity 5: Security report

Review the incident. Suggest improvements and explain how they would prevent a similar incident in the future.

Areas for improvement are:

- adherence to forensic procedures
- the forensic procedure and current security protection measures
- the security documentation.

Read the set task brief and evidence items 1–6 inclusive when answering the question.

Save your completed security report as a PDF in your folder for submission as **activity5_securityreport_[Registration number #]_[surname]_[first letter of first name]**

You are advised to spend 2 hours on this activity.

(Total for Activity 5 = 20 marks)

TOTAL FOR TECHNICAL LANGUAGE IN PART B = 3 MARKS
TOTAL FOR PART B = 37 MARKS